REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-22, 23-25, 27, 56-64, 66-76, and 79-83 are pending in the application. The Examiner additionally stated that claims 1-22, 23-25, 27, 56-64, 66-76, and 79-83 are rejected. By this communication, claims 1 and 56 are amended. Hence, claims 1-22, 23-25, 27, 56-64, 66-76, and 79-83 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-6, 11-12, 24-25, 27, 56-60, 66, and 79-83 under 35 U.S.C. 103(a) as being unpatentable over Kessler et al., U.S. Patent 6,789,147 (hereinafter, Kessler) in view of Best, U.S. Patent 4,278,837, (hereinafter, Best). Applicant respectfully traverses the Examiner's rejections.

Regarding claims 1 and 56, the Examiner noted that Kessler discloses a (microprocessor) apparatus for performing cryptographic operations comprising: fetch logic, configured to fetch an instruction flow from memory for execution by a microprocessor (col. 4, line 59-col. 5, line 36), said instruction flow comprising an instruction, configured to direct said microprocessor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate

that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 - col. 6, line 10); and a cryptography unit, disposed within execution logic in said microprocessor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55); and an integer unit, disposed within execution logic in said microprocessor and coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operation (col. 9, lines 15-20).

The Examiner conceded that the microprocessor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred narrow definition of "microprocessor" established in the specification. However, the Examiner asserted that Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, either preferably as the sole processor in a computing apparatus, or alternatively by creating a hybrid wherein a conventional microprocessor and the cryptographic coprocessor are combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 &18). The Examiner thus concluded that the claims are obvious because the technique of physically incorporating a cryptographic co-processor, such as that disclosed by Kessler, into a conventional microprocessor to create a hybrid microprocessor to be used as the CPU for a computing apparatus had clearly been long since known as being well within the ordinary capabilities of one skilled in the art.

In reply to arguments submitted by Applicant in the communication of 03/09/2008, the Examiner stated that, based upon the disclosure found within the instant specification itself wherein the term "microprocessor" is contextually defined in a manner so as to exclude co-processors (see paragraph 0017 on pages 11-12; cf. the amendment of 3/10/08, page 24, 2nd paragraph), Applicant's arguments as filed are thus found to be persuasive.

In addition, the Examiner noted for the record disagreement with Applicant's argument on page 25 of the amendment, where "Applicant also asserts that the cryptographic operation is performed atomically responsive to a cryptographic instruction, as opposed to a plurality of primitives, which is taught by Kessler." The Examiner stated that assuming this argument is applicable only to claim 1, the claim language does not in fact make a distinction of any kind as to whether the cryptographic instruction may or may not be comprised of a series of primitives, and that it is unclear from the context whether this argument could also be applied to independent claim 56. Thus, The Examiner cautioned Applicant that doing so would incur a rejection under 35 USC 112, 2nd paragraph, as that conflicts with the claim language which explicitly recites "translation logic" precisely for the purpose of implementing a cryptographic instruction as a series of primitives, just as found in the Kessler reference.

First, Applicant very much appreciates the Examiner's attention to and consideration of the arguments and amendments previously presented. Applicant also respectfully disagrees with the Examiner's characterization of the distinctions presented between a microprocessor and a coprocessor in the instant specification as being "narrow." Applicant respectfully notes that one skilled in the art would concur that there is a significant difference between a microprocessor as disclosed and a coprocessor, an example of which is taught by Kessler. One such difference is that a microprocessor is responsible for the execution of an application program, whereas a coprocessor only executes single instructions or instruction threads that are handed of to it from the main microprocessor. Consequently, to more precisely define that which is claimed as the invention, independent claims 1 and 56 are amended herein to recite that the microprocessor according to the present invention executes an application program, and the instruction directing that a cryptographic operation be performed is part of that application program, and that the microprocessor also executes the instruction to perform the cryptographic operation. Applicant believes such amendments to the claims more clearly distinguish the microprocessor according to the present invention over coprocessor implementations like that taught by Kessler.

In response to the Examiner's assertions regarding application of Applicant's argument that the cryptographic operation is performed atomically response to a cryptographic instruction and the argument's potential conflict with the claim language of claim 56, Applicant respectfully notes that even though the term "atomically" is not recited in either claim 1 or claim 56, the argument was intended to point out that whether or not a sequence of sub-operations (e.g., as recited in claim 56) are required to accomplish the cryptographic operation specified by the cryptographic instruction, it is the overall cryptographic operation itself that is atomically performed. In the case of claim 56 where a sequence of sub-operations are required, atomic performance of the specified cryptographic operation implies that all of the sub-operations are performed atomically. To this point, Kessler fails to provide such a teaching.

Regarding the specific points of rejection in the instant Office Action, Applicant respectfully disagrees with the Examiner's characterization of claims 1 and 56 and of the teachings of Kessler and Best for the following reasons.

First, notwithstanding disputation of the Examiner's assertion that Applicant's disclosure of a microprocessor is "narrow," Applicant appreciates the Examiner's note of the distinction between the coprocessor of Kessler and the microprocessor according to the present invention. Applicant believes there to be clarified distinction added by the amendments submitted herewith, as noted above.

Applicant also observes that since Kessler does not teach a microprocessor capable of fetching an instruction that 1) is part of an application program being executed by the microprocessor, and 2) that prescribes that the microprocessor perform a cryptographic operation, what is thus evident to one skilled in the art by combining the teachings of Kessler and Best remains to be argued.

As noted above, the Examiner has argued that a combination of the teachings of Kessler and Best results in the invention recited in claims 1 and 56 because "Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, either preferably as the sole processor in a computing apparatus, or alternatively by creating a hybrid wherein a conventional microprocessor and the

cryptographic coprocessor are combined into one single, indivisible microprocessor that behaves in exactly the manner as the 'microprocessor' of the instant application (col. 19, lines 20-60; Figures 17 &18), thus concluding that the claims are obvious because the technique of physically incorporating a cryptographic co-processor, such as that disclosed by Kessler, into a conventional microprocessor to create a hybrid microprocessor to be used as the CPU for a computing apparatus had clearly been long since known as being well within the ordinary capabilities of one skilled in the art.

Respectfully, Applicant disagrees in several respects with the Examiner's characterization of Best and how such teaching may be combined with that taught by Kessler. First, at a summary level, Best teaches a special purpose microprocessor that is capable of executing an application program which is stored in memory in encrypted form. That is, the microprocessor fetches portions of the enciphered application program, decrypts the enciphered portions into instructions, and then executes the instructions. In contrast to that recited in claims 1 and 56, the microprocessor of Best does not teach, contemplate, or allude to a cryptographic instruction, wherein said cryptographic instruction prescribes one of the cryptographic operations. Rather, Best teaches a technique for decrypting and executing instructions in a program, where that which the instructions prescribe is not specified. In addition, Applicant agrees that Best suggests in the discussion with reference to FIGURES 17 and 18 that a hybrid circuit on a ceramic substrate can be provided, where the hybrid circuit on the ceramic substrate consists of a prior art microprocessor chip coupled to another chip that includes a deciphering circuit.

But Applicant respectfully disputes Best's assertion that his hybrid circuit would perform as a whole like a conventional microprocessor except for the fact that the program it executes is in cipher, for Best does not address any performance attributes whatsoever. Thus, one skilled would conclude from Best's teaching is that one technique for protecting a program's contents from tampering would be to encipher the program, store it in memory, and employ a hybrid circuit as described above to execute the program—that is, if timely execution of the program were of no consequence.

Furthermore, Applicant disagrees with the Examiner's assertion that a hybrid circuit on a ceramic substrate consisting of two separate devices would lead one skilled in the art to combine Kessler's cryptographic coprocessor and Best's deciphering circuit to yield that microprocessor according to the present invention as recited in claims 1 and 56. This is because combining Kessler's cryptographic coprocessor and Best's deciphering circuit would yield, at best, a hybrid circuit that is capable of executing enciphered versions of Kessler's security primitives. Consequently, Applicant respectfully disagrees with the Examiner's assertions that a combination of Kessler and Best would yield that which is recited in claims 1 and 56. Although hybrid devices are admittedly prior art, a hybrid circuit as noted above is all that can be inferred from a combination of Kessler and Best. But the microprocessor as recited in claims 1 and 56 executes an application program having a cryptographic instruction therein that prescribes one of a plurality of cryptographic operations. Kessler in combination with Best lacks such an instruction.

In view of the above points, Applicant respectfully requests that the rejections of claims 1 and 56 be withdrawn.

With respect to claims 2-6, 11-12, 24-25, 27, 56-60, 66, and 79-83, these claims depend from claims 1 and 56 as appropriate, and add further limitations that are neither anticipated nor made obvious by Kessler, Best, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6, 11-12, 24-25, 27, 56-60, 66, and 79-83.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 7-10 and 61-64 under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Best, as noted above, and further in view of "Applied Cryptography, 2nd Edition."

Applicant respectfully traverses the Examiner's rejections and notes that claims 7-10 and 61-64, depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 7-10 and 61-64.

The Examiner additionally rejected claims 13-22 and 67-76 under 35 U.S.C. 103(a) as being unpatentable over Kessler and further in view of Johns-Vano et al. (U.S. Patent 6,026,490). Applicant respectfully traverses and notes that claims 13-22 and 67-76 depend from claims 1 and 56, respectively, and add further limitations over that subject matter which is argued above as being allowable over the prior art of record. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 13-22 and 67-76.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-22, 23-25, 27, 56-64, 66-76, and 79-83 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

09/04/2008

Date: _____